Application-aware Targeted LDP

draft-esale-mpls-app-aware-tldp-01

Santosh Esale (sesale@juniper.net)
Raveendra Torvi (rtorvi@juniper.net)
Chris Bowers (cbowers@juniper.net)
Luay Jalil (luay.jalil@verizon.com)
Uma Chunduri (uma.chunduri@ericsson.com)
Zhenbin Li (lizhenbin@huawei.com)

IETF-91 (Honolulu)

speaker: Santosh Esale

What is this draft about

- Initiating and responding LSR are made aware of targeted LDP application that needs a tLDP session

  Benefits:
  - Establishment of automatic tLDP session based on negotiated targeted LDP applications
  - Establishment of limited number of tLDP sessions for certain automatic applications
  - Targeted application is mapped to LDP FEC elements to advertise only necessary FEC label bindings over the session

Protocol changes

- Advertise and negotiate targeted applications capability (TAC) during tLDP session initialization
- The TAC TLVs capability data consists of one or more targeted application element (TAE) each pertaining to unique targeted application
- On the receipt of a valid TAC TLV, an LSR must generate its own TAC TLV with TAEs
- If there is at least one TAE common between the TAC TLV it has received and its own, the tLDP session proceed to establishment as per RFC 5036. If not, a LSR sends a 'Session Rejected/Targeted Application Capability Mis-Match' message to the peer and close the session

New in version 01

- Additional co-authors
- New use case – mLDP node protection
- Added examples of application capability negotiations
- Terminology changed : Sender/Receiver LSR → Initiating/Responding LSR

Use cases

1. Remote LFA

2. FEC 129

3. LDP over RSVP tunneling

4. mLDP node protection

Next steps

- Summary
  - 01 version addresses all the received comments
  - Draft addresses real deployment use-cases
- The authors would like to request a working group adoption